



## ■ ■ ■ ADMINISTRATION GUIDE

Lifetime Key Management  
Server Software 2.5

# security

Decru Lifetime Key Management Guide

Copyright © 2003-2007 Decru, Inc. All rights reserved.

Part number: 30-000191 A0 v 2.5 022007

No part of this manual may be reproduced in any form or any means without the prior written permission of Decru, Inc.

JRE and all Java-based marks are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries.

Copyright© 2005 Sun Microsystems, Inc. All Rights Reserved.

This software is provided "AS IS," without a warranty of any kind. ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE HEREBY EXCLUDED. SUN MICROSYSTEMS, INC. ("SUN") AND ITS LICENSORS SHALL NOT BE LIABLE FOR ANY DAMAGES SUFFERED BY LICENSEE AS A RESULT OF USING, MODIFYING OR DISTRIBUTING THIS SOFTWARE OR ITS DERIVATIVES. IN NO EVENT WILL SUN OR ITS LICENSORS BE LIABLE FOR ANY LOST REVENUE, PROFIT OR DATA, OR FOR DIRECT, INDIRECT, SPECIAL, CONSEQUENTIAL, INCIDENTAL OR PUNITIVE DAMAGES, HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY, ARISING OUT OF THE USE OF OR INABILITY TO USE THIS SOFTWARE, EVEN IF SUN HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Portions of this product are derived from FreeBSD, which is copyrighted by FreeBSD.

Copyright © 1994-2005 FreeBSD, Inc. All rights reserved.

Software derived from copyrighted material of FreeBSD is subject to the following license and disclaimer:

Redistribution and use of the software in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE FREEBSD PROJECT "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE FREEBSD PROJECT OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young.

This product includes software developed by the OpenSSL project for use in the OpenSSL Toolkit.

## **TRADEMARK NOTICE**

Decru®, Decru DataFort™, Cryptainer™, CryptoShred™, Lifetime Key Management™ software, the Decru logo and/or any Decru products or services referenced herein are trademarks and/or service marks of Decru, Inc. and may be registered in certain jurisdictions. All other product names, company names, marks, logos and symbols are trademarks or registered trademarks of their respective owners.



## ■ ■ ■ ■ CONTENTS

|                                                     |           |
|-----------------------------------------------------|-----------|
| <b>Decru Lifetime Key Management Software</b>       | <b>5</b>  |
| DataFort and LKM Server Key Limits                  | 6         |
| LKM Server Software Installation                    | 7         |
| System Requirements                                 | 7         |
| Preparing Microsoft SQL Server for LKM Installation | 8         |
| Installing LKM Software                             | 9         |
| Initial Configuration                               | 10        |
| Accessing LKM Software                              | 10        |
| Managing the LKM Server                             | 11        |
| Managing DataFort Backups to LKM                    | 11        |
| Security Policy                                     | 11        |
| <b>LKM Software</b>                                 | <b>12</b> |
| The LKM Display                                     | 13        |
| E-Series DataFort Display                           | 14        |
| FC-Series DataFort Display                          | 15        |
| Summary of Menus and Options                        | 17        |
| <b>LKM Key Archiving</b>                            | <b>19</b> |
| Overview of Recovery Functions                      | 20        |
| Generating a Recovery Key Archive                   | 21        |
| Generating Cryptainer Key Files                     | 23        |
| Key Translation Option                              | 25        |
| Translating All Cryptainer Keys                     | 25        |
| Translating Individual Keys                         | 26        |
| After Cryptainer Restoration                        | 26        |
| Key Translation from Previous LKM Versions          | 26        |
| Importing and Exporting Cryptainer Keys             | 28        |
| Creating a DataFort Clone                           | 28        |
| Exporting Cryptainer Keys                           | 28        |
| Importing Exported Cryptainer Keys                  | 28        |
| <b>LKM Management</b>                               | <b>29</b> |
| Managing the LKM Database                           | 30        |
| Importing the LKM Database                          | 30        |
| Exporting LKM Database                              | 30        |
| Syncing LKM Servers                                 | 31        |
| Zeroizing LKM Database                              | 31        |
| Managing LKM Ports                                  | 31        |
| Testing LKM Server Ports                            | 31        |
| Configuring the SSL Connection                      | 32        |
| Requiring SSL                                       | 33        |
| Configuring LKM Server Ports                        | 33        |

|                                                       |           |
|-------------------------------------------------------|-----------|
| DataFort Management                                   | 34        |
| Saving Latest DataFort Configuration Database to File | 34        |
| Deleting DataFort Records                             | 34        |
| Deleting a DataFort from LKM                          | 34        |
| Marking a DataFort Inactive                           | 35        |
| Opening DataFort WebUI                                | 35        |
| Viewing DataFort Properties                           | 35        |
| Changing the DataFort Backup Interval                 | 36        |
| Deleting a Cryptainer from LKM                        | 36        |
| Identifying Recovery Cards                            | 36        |
| <b>LKM Troubleshooting</b>                            | <b>37</b> |
| <b>Index</b>                                          | <b>38</b> |

## ■ ■ ■ ■ 1 **DECRU LIFETIME KEY MANAGEMENT SOFTWARE**

The Decru DataFort™ appliance secures data at rest by encrypting it with strong algorithms and storing it in Cryptainer vaults™. Decru Lifetime Key Management™ (LKM) software provides a way to manage encryption keys for multiple DataFort appliances, ensuring encryption key availability for the life of secured data. LKM centralizes two functions that make permanent data accessibility possible:

- Maintaining Cryptainer Key and DataFort configuration information
- Under special circumstances, providing tools for decrypting encrypted data

LKM software allows a security administrator to upload, view, manage and save DataFort configuration and key information. When used in combination with the separate Decru Decryption Software (DDS), LKM can enable authorized administrators to decrypt data outside of DataFort.

Configuring DataFort appliances to send configuration information to LKM ensures that encryption keys will be available over the long term. Once configured to send backups to LKM, a DataFort appliance or cluster can send configuration and key data to LKM.

This chapter includes the following topics:

- [DataFort and LKM Server Key Limits](#)
- [LKM Server Software Installation](#)
- [Initial Configuration](#)
- [Managing the LKM Server](#)

## DATAFORT AND LKM SERVER KEY LIMITS

An LKM server is a Windows computer running the LKM server software. One LKM server supports multiple DataFort appliances or clusters. Up to four LKM servers can be used for backup support. Consider [DataFort and LKM Server Key Limits](#) when determining the number of primary LKM servers necessary in your environment.

Keys are generated when Cryptainers are created, rekeyed or translated from one DataFort to another. When configured to do so, DataFort sends all keys to LKM to be archived. Since there are limits on the number of keys the DataFort configuration database can contain, there is an option to purge keys upon backup to LKM. This will increase available space on DataFort for new keys, and allow LKM to handle purged and active keys separately, increasing the number of keys the LKM server can manage.

The number of DataFort appliances and LKM servers required for a given enterprise will be determined by the frequency of key generation. In an environment where keys are generated often (for example where new backup tapes are being generated each day) it may be necessary to increase the number of LKM servers in the enterprise. Additional LKM servers may be needed in a large configuration with frequent key generation. When planning your installation, keep the following in mind:

**TABLE 1: KEY LIMITS**

| Item                               | Limit                        | Information                                                                                                                                                                                                                                    |
|------------------------------------|------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Keys per DataFort                  | 4500 for NAS<br>8000 for SAN | If not manually purged, the DataFort appliance will purge keys from the configuration database when the limit is reached. Issue the <code>keyman cryptainer list</code> command at the DataFort CLI to see the number of keys in the database. |
| DataFort appliances per LKM server | 32                           | Each DataFort appliance is counted towards this limit, regardless of whether it is in a cluster or not.                                                                                                                                        |
| DataFort appliances per cluster    | 2 for NAS<br>8 for SAN       | Calculate the number of keys as 8000 per DataFort in the cluster.                                                                                                                                                                              |
| Keys per LKM server                | 64000 active<br>64000 purged | When backing up to LKM from DataFort, opt to purge deleted keys upon backup. This will allow for more room to store keys in LKM. See the <i>DataFort Administration Guide</i> for details.                                                     |

Use the limits outlined in [Table 1](#) to help determine how many LKM servers are needed, and how often keys should be purged to LKM. [Table 2](#) provides an example of high frequency key generation in a SAN environment.

**TABLE 2: EXAMPLE OF HIGH FREQUENCY KEY GENERATION**

| Key Generation                       | Total |
|--------------------------------------|-------|
| Keys Generated Per Tape              | 1     |
| Tapes Generated Per Day              | 4     |
| DataFort Appliances in Cluster       | 8     |
| Keys Generated Per Day               | 32    |
| Keys in LKM Server                   | 64000 |
| Days Before LKM Key Limit is Reached | 2000  |

# LKM SERVER SOFTWARE INSTALLATION

Install the LKM server software on a Windows PC meeting the LKM server [System Requirements](#). The default setup for the LKM installs MySQL to store the key database. The LKM server can be configured to use Microsoft SQL instead.

See the following topics:

- [System Requirements](#)
- [Preparing Microsoft SQL Server for LKM Installation](#)
- [Installing LKM Software](#)

## SYSTEM REQUIREMENTS

All LKM servers should be dedicated machines used only for LKM and no other services. These servers should be regularly inspected and patched, and physical access should be controlled. LKM software relies on the correctness of the server's operating system to authenticate the LKM administrator and to protect LKM from unauthorized tampering. Be sure that no hostile process or entity compromises an LKM server.

**Note:** Using a DataFort Management Station as an LKM server is not recommended.

TABLE 3: SOFTWARE SPECIFICATIONS

| Operating System (one of the following) | Browser                          |
|-----------------------------------------|----------------------------------|
| Windows XP                              | Internet Explorer, v6.0 or later |
| Windows 2000                            |                                  |
| Windows Server 2003                     |                                  |
| Windows Server 2000                     |                                  |

TABLE 4: HARDWARE SPECIFICATIONS

| Hardware                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2.8 Ghz Pentium                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| 1GB RAM                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| 2GB free hard drive space. LKM servers supporting multiple DataFort appliances may require more disk space. During installation you can opt to specify a different server to contain the database.                                                                                                                                                                                                                                                                                                                                                  |
| A fixed IP address accessible via Ethernet to all DataFort appliances that will use LKM. DataFort appliances will send automated backups to this address.                                                                                                                                                                                                                                                                                                                                                                                           |
| 256kb connection for any remote LKM Server                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| An available USB port for the smart card reader from Decru                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| A CD drive for installing software                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Available server ports: By default LKM server ports are set to 15362 and 15363. These ports should be available to allow automated communication between the LKM server and DataFort appliances. If using a Windows XP server, add the ports used by LKM to Windows Firewall. Open Windows Firewall and click the Exceptions tab. Add ports 15362 and 15363 for clear communication and ports 15372 and 15373 for SSL using the Add port button. See <a href="#">Managing LKM Ports</a> on page 31 if you need to change the default port settings. |

## PREPARING MICROSOFT SQL SERVER FOR LKM INSTALLATION

LKM can use a MySQL database to store data (this is the default), or it can be configured to use a Microsoft SQL Server. This designation is made during the installation wizard as described in [Installing LKM Software](#). In order to configure LKM to use a Microsoft SQL Server as the database, the server must be prepared before installing LKM. LKM supports Microsoft SQL 2000 and Microsoft SQL 2005.

**Note:** The default installation using MySQL does not require this step. For ordinary installation, skip to [Installing LKM Software](#) on page 9.

1. From the left pane of the Microsoft SQL Server Enterprise Manager, expand the Microsoft SQL Servers entry in the Console Root tree.
2. Expand the entry for your SQL Server installation and right-click the Databases directory.
3. Select New Database from the right-click menu. Create a database called Decru and click OK.
4. Right-click the Security directory under your SQL Server installation and right-click Logins.
5. Select New Login from the right-click menu.
6. Enter a name of your choice for this user. You will be prompted for this information during LKM installation.
7. Select the SQL Server Authentication button, and enter a password for this user. You will be prompted for this information during LKM installation.
8. Specify the Decru database as the default for this login by selecting it from the Database pull-down menu. Click OK.
9. Confirm the new password.
10. Expand the entry for your SQL Server installation, and expand the Databases directory.
11. Expand the Decru database directory and right-click the Users entry. Select New Database User from the right-click menu.
12. Select the new user from the pull-down menu of login names.
13. Check the boxes that will assign the following permissions to the user: public, db\_owner, db\_accessadmin, db\_securityadmin, db\_ddladmin, db\_backupoperator, db\_datareader, db\_datawriter.
14. Click OK to complete the operation.
15. Right-click your SQL Server entry in the left pane and select Properties.
16. Check the Autostart SQL Server Agent box at the bottom of the General tab.
17. Select the Security tab and be sure that the authentication button for SQL Server and Windows is selected.
18. Click OK.
19. Continue with [Installing LKM Software](#).

## INSTALLING LKM SOFTWARE

1. Insert the DataFort CD in a drive on the LKM server. The CD will run automatically.
2. Click the Lifetime Key Management installer link. When prompted by the File Download screen to open or save the file, click the Open button to open the file.
3. Follow the prompts to start the installer and accept the terms of the license agreement.
4. Enter the LKM license key provided by Decru and click Next.
5. Click next to allow the system to be checked for software requirements.
6. Specify the installation directory or use the default. Click Next.
7. Click Install to begin installation.
8. Specify the database type to use with LKM (MySQL or Microsoft SQL Server) and click Next.

**MySQL:** This is the default installation. It will place MySQL 4.1.x on the server.

- Enter a database user name of your choice.
- Enter a password for that user.
- Confirm the user password by entering it again.
- Set the path to the data directory, or accept the default location and click Next.

**Microsoft SQL Server:** Select this if a Microsoft SQL Server has been configured for use with LKM as described in [Preparing Microsoft SQL Server for LKM Installation](#). Enter the server information:

- Enter the IP address of the Microsoft SQL Server.
  - Enter the user name (the same user name that was added to the Microsoft SQL Server).
  - Enter the user password (the same password that was added to the Microsoft SQL Server).
9. Follow the prompts to start the smart card reader installer (if the smart card reader driver is not already installed. Accept the license agreement, and select the model number of your smart card reader. The model number can be found on the underside of the smart card reader.
  10. Select “Yes, I want to restart my computer now” and click Finish to complete installation.
  11. After the LKM server reboots, the LKM Service starts automatically. Click the LKM desktop icon or select **Start > Programs > Decru > Lifetime Key Management** to view LKM.

## INITIAL CONFIGURATION

---

Follow instructions in the [DataFort Administration Guide](#) for your model of DataFort appliance to configure DataFort to send automatic backups to LKM. You must specify the LKM server or servers using the DataFort WebUI before LKM can function.

- Specify LKM settings for each DataFort or DataFort cluster as described in the [DataFort Administration Guide](#) that came with your DataFort.
- Leave the LKM server or servers running at all times. LKM receives updates from DataFort appliances whether or not the administrator is logged into the server.

## ACCESSING LKM SOFTWARE

After LKM has been specified for a DataFort or DataFort cluster, check the LKM UI to verify that LKM archives are being updated. The UI offers drop-down menus for key functions, and the left pane lists DataFort appliances that have backed up key data to LKM. Status is shown at the base of the screen.

1. To start the LKM UI, click the LKM program icon on the Windows desktop, or choose **Start > Programs > Decru > Lifetime Key Management**.
2. Click the DataFort Appliances folder in the left pane. The list will include all DataFort appliances configured to use this LKM server. When you select a DataFort appliance, the right pane displays all of its associated Cryptainers. All Recovery Cards connected with this DataFort are also added to the Recovery Cards List.
  - If you don't see a DataFort that was recently configured to use LKM, right-click DataFort Appliances in the left frame, and choose Refresh List. Before DataFort appliances will appear in the LKM UI, they must be configured to send backups to LKM.
  - If a DataFort has been configured to use LKM, but does not appear in the list of DataFort Appliances, make sure the communication ports specified on the LKM server are correct. See [LKM Troubleshooting](#).
3. Right-click a DataFort and choose Properties. The DataFort Properties dialog displays information about the DataFort, including the date and time of the most recent configuration update. The date and time should correspond approximately to the most recent configuration changes.
4. After LKM displays a DataFort in its list of DataFort Appliances, assemble the Recovery Officers and create a Recovery Key Archive for the DataFort. See [Generating a Recovery Key Archive](#).

## MANAGING THE LKM SERVER

---

The LKM server software has two components: the Lifetime Key Management Windows Service, and the LKM UI. Both components communicate with the LKM internal database. The Lifetime Key Management service starts automatically when the LKM server is booted, and runs as long as the server is on, allowing the server to receive updates from DataFort appliances.

In common with other Windows Services, the Lifetime Key Management service can be manually stopped and restarted. To reset the service manually, open the Administrative Tools under Control Panel and choose Services. Select Decru Lifetime Key Management Service and choose Stop from the Action menu. To restart, select Decru Lifetime Key Management Service again and choose Restart.

The UI component is started from the Decru Lifetime Key Management desktop icon or the Start menu (**Start > Programs > Decru > Lifetime Key Management**). It provides all the LKM functions that originate from the LKM server. Multiple instances of the LKM UI can be run at the same time.

## MANAGING DATAFORT BACKUPS TO LKM

By default the DataFort configuration database is checked every hour for changes. If certain changes to the configuration (such as the presence of new encryption keys or access controls) are found, new data will be sent to LKM. Note that the frequency of this database check can be configured. See [Identifying Recovery Cards](#) on page 36 for details.

## SECURITY POLICY

Administering LKM from the LKM server does not require special DataFort permissions or smart cards, however some procedures require a quorum of Recovery Officers and their Recovery Cards. Consider the following when planning the security policy for the LKM installation:

|                            |                                                                                                                                                                                                                                                                                                                                                                                              |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Recovery Officers</b>   | For the highest security, make sure Recovery Officers retain and do not share their Recovery Cards and passwords, or that possession of the card and possession of the password are entrusted to different individuals.                                                                                                                                                                      |
| <b>Recovery Cards</b>      | Before inserting Recovery Cards in a smart card reader connected to a Windows PC, check the computer thoroughly to make sure that no malicious code has been installed on it. You may leave the smart card reader attached to the LKM server, but for security reasons it is not advisable to leave smart cards in the reader.                                                               |
| <b>Key Archive File</b>    | As soon as a Recovery Key Archive is created, send it to a key escrow service and delete the file from local storage. Make the passphrase available to the escrow service, but do not share it with anyone else.                                                                                                                                                                             |
| <b>Cryptainer Key File</b> | The LKM server creates an internal copy of the Cryptainer Key File and deletes it automatically after use. If you need to create a Cryptainer Key file, create it for a single Cryptainer if you don't need to decrypt all the Cryptainers of a DataFort. Do not share the passphrase for a Cryptainer Key File. After it has served its purpose, be sure to delete the Cryptainer Key File. |
| <b>Key Escrow</b>          | To ensure recoverability, Recovery Key Archives, Recovery Cards, passwords and backups of the configuration database may be escrowed or placed in trusted long term storage.                                                                                                                                                                                                                 |



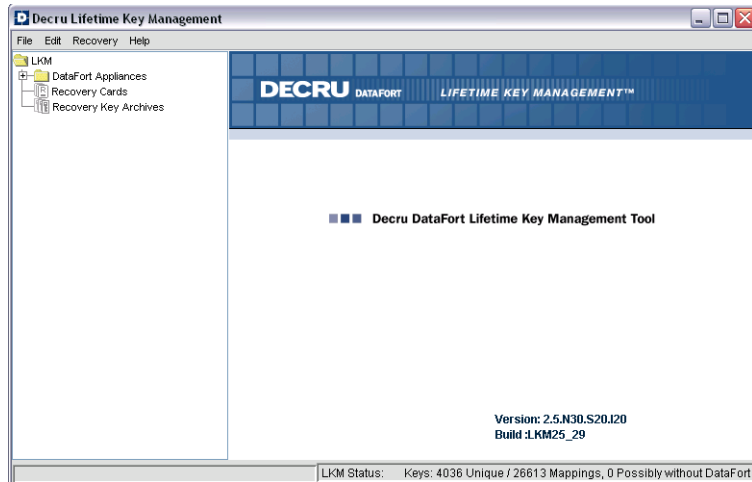
## ■ ■ ■ ■ 2 LKM SOFTWARE

The LKM server is managed using the LKM UI. This chapter includes the following topics:

- [The LKM Display](#)
- [Summary of Menus and Options](#)

## THE LKM DISPLAY

To start the LKM UI, click the LKM program icon on the Windows desktop, or choose **Start > Programs > Decru > Lifetime Key Management**.



The left pane displays:

- DataFort Appliances
- Recovery Cards
- Recovery Key Archives

Right-clicking an object displays a menu of commands and options available for that object. Additional commands are available from the menu bar. Information is displayed in the right pane, according to the selection in the left pane. To exit the LKM UI, choose **File > Exit**, click the Close box, or choose Close from the taskbar menu.

The lower pane status bar will display the status of LKM and the number of encryption keys in use (this includes tape and Cryptainer keys). Keys are distinguished as mapped or unique. The mapping number indicates the total number of Cryptainers mapped to a given key, while the unique key number indicates the total number of keys.

Once DataFort configurations have been backed up to LKM, the display shows the contents of the LKM database.

**DataFort Appliances** When **DataFort Appliances** is selected in the left pane, the right pane displays DataFort appliances that are configured to perform backups to LKM. For each DataFort, the right pane lists the DataFort ID, the DataFort Name, the Type (DataFort model and network type), and the optional description given to the appliance using the DataFort WebUI.

- Individual DataFort

When a DataFort appliance is selected in the left pane, the right pane shows a cumulative list of Cryptainers for the selected DataFort. The display can be expanded to show the view options for that type of DataFort. An E-Series DataFort will show NAS and iSCSI view options, and the FC-Series DataFort will show disk and tape view options.
- Individual Cryptainer

Cryptainer entries are color-coded: **blue** by default, **gray** if the Cryptainer has been deleted from a DataFort configuration, and **red** if the Cryptainer was translated from a different DataFort.
- Recovery Cards

LKM displays all of the Recovery Cards associated with a DataFort, including label and Security Domain information.
- Recovery Key Archives

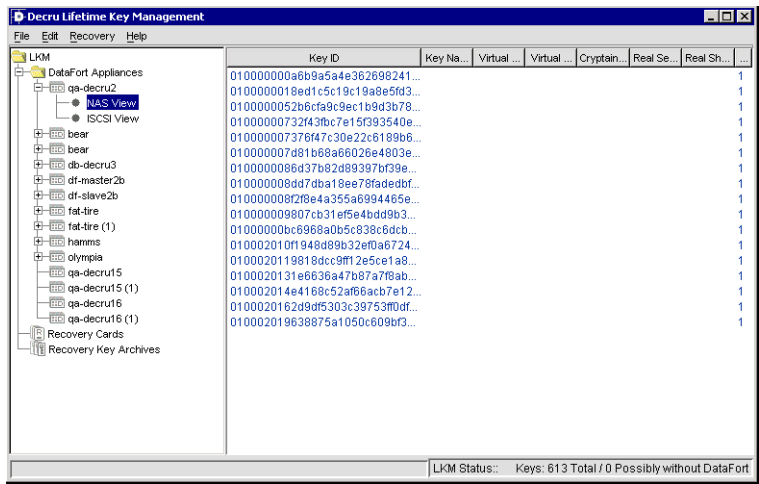
The right pane lists all Recovery Key Archives created with the current instance of LKM. The listing includes the Key Archive ID (a sequential autonumber), the creator's comment, DataFort Name, Master Key ID, and time of creation. The list indicates only that a Recovery Key Archive was created; it cannot be used to retrieve the Recovery Key.

E-SERIES DATAFORT DISPLAY

The E-Series DataFort supports the creation of Cryptainers in the NAS and iSCSI environment. LKM will display two entries for an E-Series DataFort: [NAS View](#) and [iSCSI View](#). Each view will show the list of Cryptainers created by that DataFort in the NAS or iSCSI environment.

NAS View

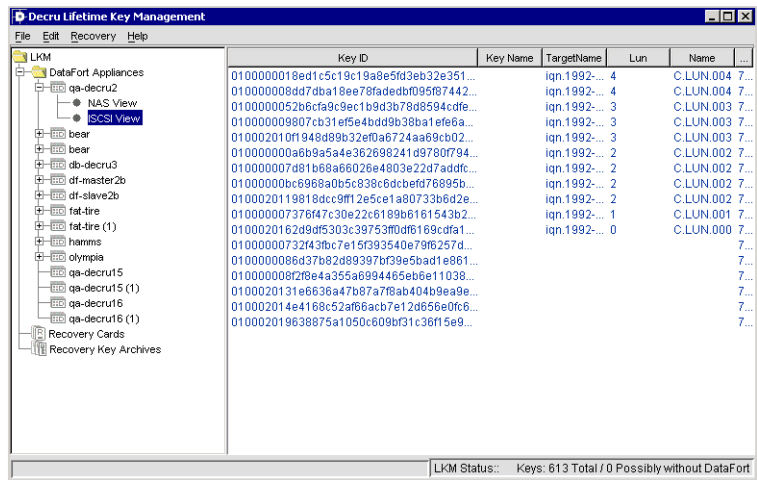
For each Cryptainer, LKM displays the unique Cryptainer Key ID, Key Name, Virtual Server, Virtual Share name, Cryptainer Name, Real Server name, Real Share name and Key Version. The Key Version will be 1 unless the Cryptainer has been rekeyed.



LKM interface with E-Series appliance selected, NAS view

ISCSI View

For each Cryptainer, LKM displays the Key ID, Key Name, name of the target where the Cryptainer is stored, the LUN number and name and Creation Date. The creation date reflects the date of encryption, and will change if the Cryptainer is rekeyed.



LKM interface with E-Series appliance selected, iSCSI view

FC-SERIES DATAFORT DISPLAY

The FC-Series DataFort supports the creation of Cryptainers in the SAN tape and disk environments. LKM will display two entries for an FC-Series DataFort: [Tape View](#) and [Disk View](#). Each view will show the list of Cryptainers created by that DataFort on tape or disk storage.

Tape View

For each Cryptainer, LKM displays the Key ID, Key Name, Pool Label, Media Label, Name, Creation Date, Expiration Date and Key Type. Expiration dates for keys can be set using the DataFort WebUI as described in the [DataFort Administration Guide](#). Once a key's expiration date arrives, the key will automatically be deleted from LKM. Tape keys generated from a per-pool pool will show up in LKM as Pool type keys and have no specific Media ID. However, tape keys from per-tape pools will show up as Tape type and will have both Pool and Media IDs.

Depending on the way DataFort key policy is set, the same key may be used for multiple tapes (such as tapes in the same pool). Since LKM only stores key information, only one key will be displayed for those tapes, even though each tape will have its own entry in the DataFort configuration database and will be visible in the DataFort UI.

The latest key that is sent to LKM by DataFort will overwrite previous keys with the same ID. If several tapes use the same key, you will only see one instance of that key in LKM, but all tapes using that key can be restored by LKM if necessary.

| Key ID                          | Key Name | Pool Label | Media Label | Name      | Creation Date | Expiration Date |
|---------------------------------|----------|------------|-------------|-----------|---------------|-----------------|
| 0100020103e9ec84ce62eba25b...   | 7        | 0101L2     |             | 7/22/0... |               |                 |
| 010002010d37fd11241c0c7f840...  | 7        | 0100L2     |             | 7/25/0... |               |                 |
| 010002011e345010bdd6a0f4af4...  | 7        |            | 7           | 7/22/0... |               |                 |
| 01000201f24141c4b842e10929...   | 7        | 0903L3     |             | 7/28/0... |               |                 |
| 01000201fae08ef1b358487fdd0d... | 7        | 8AHLR2     |             | 7/25/0... |               |                 |
| 0100020113228fa93fe5cefe3e...   | 5        | 0100L2     |             | 7/27/0... |               |                 |
| 010002012e2f417ee385df6668d...  | 5        | 0101L2     |             | 7/27/0... |               |                 |
| 01000201338fba263754e2475d...   | 5        | 0101L2     |             | 7/27/0... |               |                 |
| 01000201ee0ed1229332f231b6...   | 5        |            | 5           | 7/27/0... |               |                 |
| 01000201004150003c22fd3cf3d...  | 3        | A00043     |             | 7/26/0... |               |                 |
| 0100020100952d6ff2289aa9a0...   | 3        | A00044     |             | 7/26/0... |               |                 |
| 01000201009b5f0b0145596f9a8...  | 3        | A00029     |             | 7/27/0... |               |                 |
| 0100020100d9fca9a62af865846...  | 3        | A00038     |             | 7/26/0... |               |                 |
| 01000201012ead345da02c4a64...   | 3        | A00029     |             | 7/26/0... |               |                 |
| 0100020101f69a739b7a294338...   | 3        | A00041     |             | 7/26/0... |               |                 |
| 010002010558bd0ae127ade290...   | 3        | A00029     |             | 7/27/0... |               |                 |
| 0100020107ae177f5c6ac3697ec...  | 3        | A00001     |             | 7/22/0... |               |                 |
| 010002010a1ecba3e73eaf7a9a...   | 3        | A00007     |             | 7/26/0... |               |                 |
| 010002010a3fc372ae6c4028d1b...  | 3        | A00007     |             | 7/26/0... |               |                 |
| 010002010a3f65fabaf642df8a9...  | 3        | A00014     |             | 7/26/0... |               |                 |
| 010002010b4722d2aeb401098...    | 3        | A00070     |             | 7/27/0... |               |                 |
| 0100020110791c974988a2c2bc...   | 3        | A00029     |             | 7/27/0... |               |                 |
| 010002011132ac12caa82907b1...   | 3        | A00031     |             | 7/26/0... |               |                 |
| 010002011509ae1d83cf62b736...   | 3        | A00037     |             | 7/26/0... |               |                 |
| 0100020117ebdd565b9a4b3661...   | 3        | A00029     |             | 7/26/0... |               |                 |

LKM Status: Keys: 613 Total / 0 Possibly without DataFort

LKM interface with an FC appliance selected, Tape view

## Disk View

For each Cryptainer, LKM displays the Key ID, Key Name, Host Port WWN, Port WWN, LUN, Cryptainer Name, and Creation Date. The creation date reflects the date of encryption, and will change if the Cryptainer is rekeyed.

| Key ID                             | Key Name | Host Port WWN | Port WWN   | Lun | Name | Creation Date |
|------------------------------------|----------|---------------|------------|-----|------|---------------|
| 010002011be4b3c814f05a527d2ad9...  | ...      | ...           | 50.06.0... | 8   | 1    | ...           |
| 010002012a4510df950b5c8d3124b3...  | ...      | ...           | 50.06.0... | 6   | 1    | ...           |
| 0100020130d163825d98b7cc7d00ba...  | ...      | ...           | 50.06.0... | 13  | 1    | ...           |
| 010002014bee071198ade06c6288e8...  | ...      | ...           | 50.06.0... | 7   | 1    | ...           |
| 0100020166828ec84761903f93f9764... | ...      | ...           | 50.06.0... | 21  | 1    | ...           |
| 010002017a2b6c78d2363ba321f7ad...  | ...      | ...           | 50.06.0... | 10  | 1    | ...           |
| 010002017feda87569e1716163d75f...  | ...      | ...           | 50.06.0... | 12  | 1    | ...           |
| 01000201a2a506bdefe884a496bd4c...  | ...      | ...           | 50.06.0... | 11  | 1    | ...           |
| 01000201d7d19149c70c06c4a25471...  | ...      | ...           | 50.06.0... | 20  | 1    | ...           |
| 01000201f59a0f679e6bcfd352dbb12... | ...      | ...           | 50.06.0... | 8   | 1    | ...           |
| 01000201fcb72a8a6292a93e93d734...  | ...      | ...           | 50.06.0... | 9   | 1    | ...           |
| 01000000d8062ca832892e8f37e62a...  | ...      | ...           | 50.03.0... | 0   | 1    | ...           |
| 01000000dfb1e13a6cde0f63ae0aee3... | ...      | ...           | 50.03.0... | 1   | 1    | ...           |
| 010000000acc8519f45952eff6c0d91... | ...      | ...           | 21.00.0... | 1   | 1    | ...           |
| 010000002a139ee9b82aed7efe9514...  | ...      | ...           | 21.00.0... | 0   | 1    | ...           |
| 010000005b7f51401d197be0ca9aa7...  | ...      | ...           | 21.00.0... | 1   | 1    | ...           |
| 01000000c1ab0c0bd73245dc158dc3...  | ...      | ...           | 21.00.0... | 0   | 1    | ...           |
| 01000000664df834971bce63b8e406...  | ...      | ...           | 21.00.0... | 0   | 1    | ...           |
| 01000000861fc4298913b3b42b731d...  | ...      | ...           | 21.00.0... | 1   | 1    | ...           |
| 0100000065eb3f767d43a77985f4...    | ...      | ...           | 10.00.0... | 0   | 1    | ...           |
| 01000000edd81794581acc8babec7a...  | ...      | ...           | 10.00.0... | 1   | 1    | ...           |
| 010000000634c002e33949bab0fc0c...  | ...      | ...           | 10.00.0... | 1   | 1    | ...           |
| 010000000f183667b7f453b585b17c...  | ...      | ...           | 10.00.0... | 0   | 1    | ...           |
| 01000000d808688a15974427fcaefe...  | ...      | ...           | 10.00.0... | 2   | 1    | ...           |
| 01000201004150003c22fd3cf3d9aa8... | ...      | ...           | ...        | ... | 1    | ...           |

LKM Status: Keys: 613 Total / 0 Possibly without DataFort

LKM interface with an FC appliance selected, Disk view

## SUMMARY OF MENUS AND OPTIONS

LKM menus and options are summarized in the tables that follow. [Table 5](#) lists LKM drop-down menus. [Table 6](#) lists the right-click menu options that are available in the context of an LKM item.

**TABLE 5: LKM MENUS**

| Menu Name | Drop-down Option      | Function                                                                                                                   |
|-----------|-----------------------|----------------------------------------------------------------------------------------------------------------------------|
| File      | Import                | Imports a LKM Database Export File.                                                                                        |
|           | Export                | Exports a LKM Database Export File.                                                                                        |
|           | Zeroize               | Clears the contents of the LKM database.                                                                                   |
|           | Exit                  | Quits LKM WebUI.                                                                                                           |
| Edit      | Port                  | Allows the port and SSL connections of LKM server to be configured. See <a href="#">Managing LKM Ports</a> .               |
| Recovery  | Recovery Cards        | Displays all Recovery Cards associated with configuration databases loaded into LKM.                                       |
|           | Identify Card         | Displays attributes of a Recovery Card inserted in the smart card reader. See <a href="#">Identifying Recovery Cards</a> . |
|           | Recovery Key Archives | Displays Recovery Key Archives.                                                                                            |
| Help      | Contents              | Opens the PDF file of this document.                                                                                       |
|           | About LKM             | Displays the LKM software version.                                                                                         |

TABLE 6: LKM OPTIONS IN CONTEXT

| Item                  | Name                          | Description/Function                                                                                                                                                                                              |
|-----------------------|-------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DataFort Appliances   | Refresh List                  | Refreshes the display of DataFort appliances.                                                                                                                                                                     |
| DataFort              | Export Keys                   | Export of all Cryptainer Keys to another LKM server. See                                                                                                                                                          |
|                       | Translate Keys                | Makes the selected DataFort's Cryptainers accessible to another DataFort. See <a href="#">Key Translation Option</a> . Translate Keys to 2.0/3.0 DataFort appears if the selected DataFort is an earlier version. |
|                       | Generate Key File             | Generates a Cryptainer Key file for all Cryptainer vaults associated with selected DataFort. See <a href="#">Generating Cryptainer Key Files</a> .                                                                |
|                       | Generate Recovery Key Archive | Creates a file containing a passphrase-encrypted Recovery Key. See <a href="#">Generating a Recovery Key Archive</a> .                                                                                            |
|                       | Launch WebUI                  | Opens DataFort WebUI. See <a href="#">DataFort Management</a> .                                                                                                                                                   |
|                       | Save DB                       | Creates a file of the last configuration database sent to LKM from selected DataFort. See <a href="#">Saving Latest DataFort Configuration Database to File</a> .                                                 |
|                       | Mark Inactive/Active          | Marks DataFort status. See <a href="#">Marking a DataFort Inactive</a> .                                                                                                                                          |
|                       | Delete Records                | Deletes records of the selected DataFort from LKM. See <a href="#">DataFort Management</a> .                                                                                                                      |
|                       | Refresh                       | Refreshes the Cryptainer and key list in the right pane and refreshes DataFort Properties.                                                                                                                        |
|                       | Properties                    | Displays the DataFort properties that are recorded in LKM. See <a href="#">Viewing DataFort Properties</a> .                                                                                                      |
| Cryptainer            | Export Key                    | Export Cryptainer Key to another LKM server.                                                                                                                                                                      |
|                       | Translate Key                 | Makes the selected Cryptainer accessible to another DataFort. See <a href="#">Key Translation Option</a> . Translate Key to 2.0/3.0 DataFort appears if the selected DataFort is an earlier version.              |
|                       | Generate Key file             | Generates key file for selected Cryptainer. See <a href="#">Generating Cryptainer Key Files</a> .                                                                                                                 |
|                       | Delete from LKM               | Deletes record of selected Cryptainer from LKM. See <a href="#">Deleting a Cryptainer from LKM</a> .                                                                                                              |
| Recovery Cards        | Refresh Cards List            | Refreshes the display of Recovery Cards.                                                                                                                                                                          |
| Recovery Key Archives | Refresh Archives List         | Refreshes the display of archived Recovery Key files.                                                                                                                                                             |



## ■ ■ ■ ■ 3 LKM KEY ARCHIVING

DataFort appliances encrypt and decrypt data within Cryptainers, but there are occasions when LKM software is useful in providing long-term access to encrypted data. LKM offers key archiving tools to aid in disaster recovery. This chapter includes the following topics:

- [Overview of Recovery Functions](#)
- [Generating a Recovery Key Archive](#)
- [Generating Cryptainer Key Files](#)
- [Key Translation Option](#)
- [Importing and Exporting Cryptainer Keys](#)

## OVERVIEW OF RECOVERY FUNCTIONS

---

The following situations might render data inaccessible without LKM:

- A replaced or reconfigured DataFort appliance
- Purged encryption keys that are needed again
- Data transfer from one Cryptainer to another
- Lost Recovery Cards
- Theft or destruction of the only DataFort appliance

LKM functions provide the necessary components of emergency data recovery including:

- Recovery Key Archive** A Recovery Key Archive should be created for every DataFort after it is initialized. The Recovery Key Archive is generally valid for the life of the DataFort. A new Recovery Key Archive is needed only if the DataFort is zeroized and subsequently reinitialized. The archive is used for recovering data that has been encrypted if the original DataFort is no longer available. See [Generating a Recovery Key Archive](#).
- Generate Key File** LKM can generate a Cryptainer Key File to decrypt a single Cryptainer or all Cryptainers in a DataFort configuration. [Generating Cryptainer Key Files](#) is an intermediate component of data recovery. A Cryptainer Key File is used by Decru's Data Decryption Software (DDS) to recover data. Note that a Cryptainer Key File can only be used to decrypt Cryptainers that were in LKM when the Cryptainer Key File was created. The Data Decryption Software (DDS) will decrypt a Cryptainer using a Cryptainer Key File and its passphrase.
- Translate Keys** The [Key Translation Option](#) enables all Cryptainers on a selected DataFort to be accessible from another DataFort.
- Import/Export Keys** LKM can be used to export and import Cryptainer and Tape Keys from one LKM server to another. See [Importing and Exporting Cryptainer Keys](#).

**CAUTION:** Generation of Recovery Key Archives and Cryptainer Key Files reveals the plaintext Recovery Key to the recovery software; accordingly, these processes should be executed only on a secure machine that has been scanned for viruses and preferably is not on the network. Decru recommends rebooting the machine after either process.

## GENERATING A RECOVERY KEY ARCHIVE

The Recovery Key is used to encrypt each unique Cryptainer Key in a DataFort's configuration. In the event that both a DataFort and its associated Recovery Cards are unavailable, LKM can use a Recovery Key Archive to supply the keys needed to decrypt data. To create the archive, LKM retrieves the Recovery Key from a DataFort configuration and quorum of Recovery Cards, and saves it as a passphrase-encrypted file.

**CAUTION:** Because the Recovery Key Archive file compromises the distributed security design of the DataFort System Card and Recovery Cards, a Recovery Key Archive should be created and used for only two purposes: immediate data recovery if a DataFort is no longer functioning, and placement in key escrow or another form of trusted long-term storage, for use in an emergency.

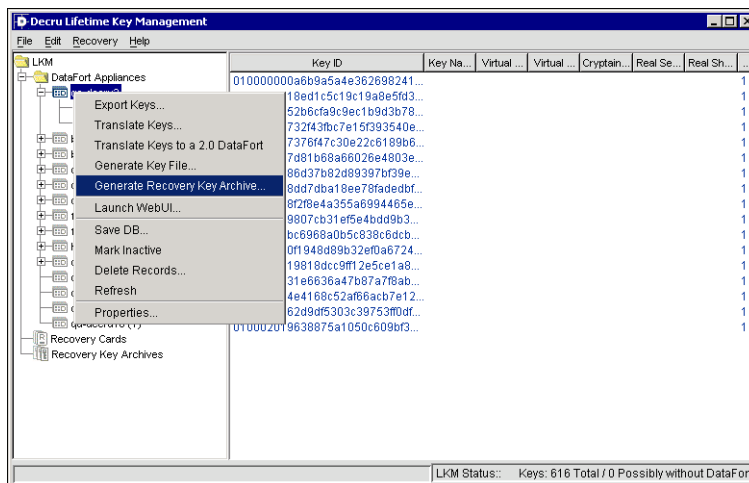
A Recovery Key Archive should be created after every DataFort is initialized in order to ensure key availability. The Recovery Key Archive is generally valid for the life of the DataFort. A new Recovery Key Archive is needed only if the DataFort is zeroized and subsequently reinitialized.

Generating a Recovery Key Archive requires:

- The quorum of Recovery Officers and Recovery Cards (as configured during DataFort setup). Each Recovery Officer will be required to present a Recovery Card and its password.
- A passphrase that the security administrator will supply in the course of generating the Recovery Key Archive to encrypt the Recovery Key Archive.

**CAUTION:** Before inserting Recovery Cards in the reader connected to the LKM server, the LKM server should be thoroughly checked for the presence of malicious code that could compromise the security of encrypted data.

1. Right-click a DataFort and choose Generate Recovery Key Archive.



You are informed of the quorum of Recovery Cards required for the selected DataFort.

2. A scrollbar lists the Recovery Cards in the Security Domain. If desired, control-click to select the particular Recovery Cards you will present to speed up the process. Click Next.
3. When prompted, a Recovery Officer should insert a Recovery Card in the smart card reader, and click OK.
4. Enter the Recovery Card password. Click Next.

The previous two steps are repeated for all the Recovery Cards in the quorum.

5. When prompted for a passphrase for the Recovery Key Archive, enter it twice and make a note of it. Click Next.
6. Enter a comment or identifying name to help identify the Recovery Key Archive, and browse or enter the path to the directory where the file should be saved.
7. Enter a descriptive filename and click Save. Click Finish.

The name of the Recovery Key Archive is added to the left frame, and to the DataFort Properties.

8. Move the Recovery Key Archive file to escrow or secure long-term storage, making sure you store the passphrase as well.

**CAUTION:** Delete every Recovery Key Archive immediately after use or submission to escrow. Do not leave Recovery Key Archive files on the LKM server or any other accessible location, as they may compromise the security of encrypted data.

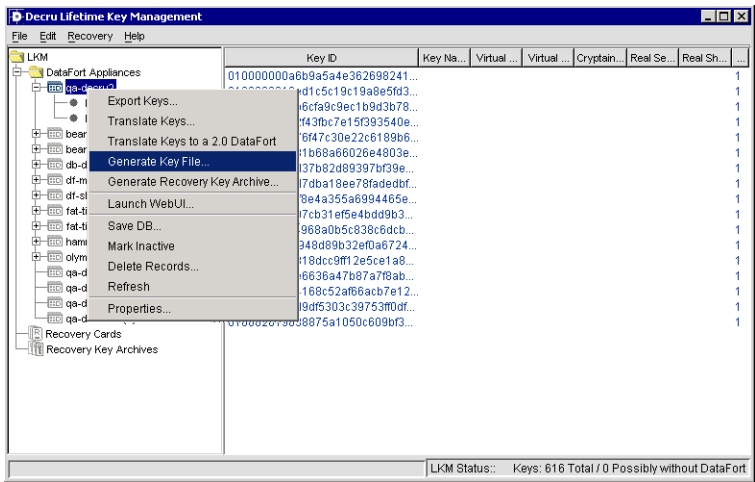
## GENERATING CRYPTAINER KEY FILES

LKM can generate a Cryptainer Key File that contains passphrase-encrypted Cryptainer Keys or tape keys. These keys allow the recovery of encrypted data under special circumstances without DataFort.

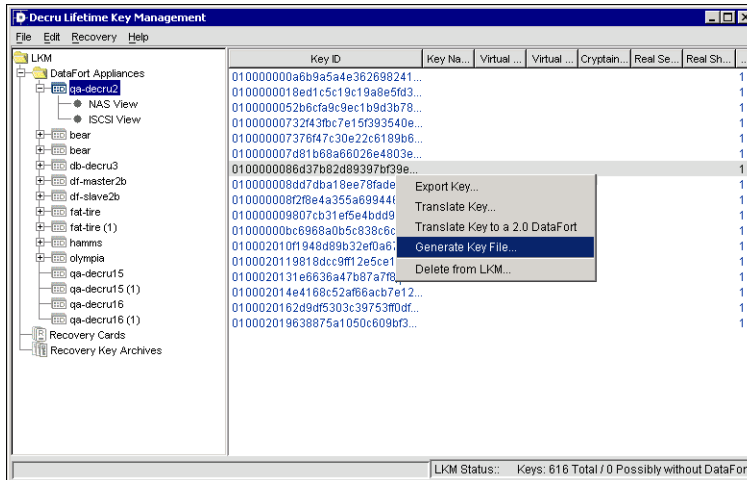
Before a Cryptainer Key can be used, the Recovery Key must be introduced into the LKM software. This is done by presenting either a quorum of Recovery Cards or a Recovery Key Archive file. In the

**CAUTION:** Before inserting Recovery Cards in the smart card reader connected to the LKM server, the LKM server should be thoroughly checked for the presence of malicious code that could compromise the security of encrypted data.

1. Generate a Cryptainer Key File for a single Cryptainer, or for all Cryptainers in a configuration database.
- To generate Cryptainer Keys for all Cryptainers associated with a DataFort, right-click the DataFort in the left pane, and choose Generate Key File. Note that such a Cryptainer Key File can only be used to decrypt Cryptainers recorded in LKM at the time the Cryptainer Key File was created.



- To generate a Cryptainer Key File for a single Cryptainer, select the DataFort in the left pane. A list of Cryptainers is shown on the right. Right-click the Cryptainer you wish to recover, and choose Generate Key file.



2. Select the method by which the Recovery Key will be introduced.
  - If you are using Recovery Cards to supply the Recovery Key, you are told how many Recovery Cards will be required. Pre-selecting the Recovery Cards that will be used speeds up the process. Recovery Officers should follow the screen prompts to insert Recovery Cards in the smart card reader and authenticate them with their passwords. Click OK.
  - Alternatively, if you are using the Recovery Key Archive to supply the Recovery Key, browse to locate the Recovery Key Archive file, and enter the Recovery Key Archive passphrase. Click Next.
3. Whether you used Recovery Cards or the Recovery Key Archive, enter a passphrase for LKM to use to encrypt the Cryptainer Key File. Enter it again to confirm, make a note of it, and click Next.
4. Browse or enter a location for storing the Key File. Enter a filename, and click Save. Record the passphrase, the filename, and the nature of the Key File so you can identify and use it later.
5. Click Finish. The Key File is stored in the designated location.

## KEY TRANSLATION OPTION

---

Key Translation transfers one or more Cryptainer or tape keys from one DataFort to another. In the event that one DataFort is unavailable or has been reassigned (for example to secure data for a different group), an administrator may transfer the Cryptainers protected by that DataFort (the source DataFort) to another DataFort (the target). Key Translation may also be used as a backup for a DataFort; it does not disable the Cryptainer Keys from the source DataFort.

Key Translation can be performed for one or more Cryptainers, and the target can be one or more DataFort appliances. Key translation can be performed for all Cryptainers at once, or one at a time.

Key Translation is initiated from the LKM server that contains key information for both the source and target DataFort appliances. It requires a quorum of Recovery Officers and Recovery Cards for both the source and target DataFort, if they are secured by different individuals and cards.

**CAUTION:** In the Key Translation process Recovery Keys as well as a Cryptainer Key are exposed to software on the LKM server. Therefore, before initiating Key Translation, the LKM server should be thoroughly checked to ensure that no malicious code has been installed on it.

After the key or keys are translated to the target DataFort, the administrator must perform a Cryptainer Restore operation on each of the translated Cryptainers, in order to make them accessible from the target DataFort. The steps are outlined below.

### TRANSLATING ALL CRYPTAINER KEYS

Key translation can be authenticated either with Recovery Cards or Recovery Key Archives. In the first case, assemble the Recovery Officers and Recovery Cards for both the source DataFort and the target DataFort. In the second case, obtain Recovery Key Archives for the source and target DataFort.

**Note:** See [Key Translation from Previous LKM Versions](#) on page 26 if translating keys from an older version of DataFort.

1. Right-click the source DataFort in the LKM UI, and choose Translate Keys.
2. From the drop-down list, choose the target DataFort. The list includes all the DataFort appliances known to the LKM server.
3. Choose the method of authenticating the Key Translation and click Next. Choose Use Recovery Cards unless you have already created a Recovery Key Archive.
  - If you choose Use Recovery Cards, LKM displays the names of the Security Domains of the source and target DataFort appliances. The quorum of Recovery Cards that will be needed (from both DataFort appliances) will be displayed. When prompted to insert Recovery Cards, Recovery Officers insert their Recovery Cards in the smart card reader, and enter their passwords.

Control-click to pre-select the cards you will present, if desired, to speed up the process. Click Next. Follow the prompts to insert each card and enter its password.

  - If you choose Use Recovery Key Archives, browse or enter the path to the Recovery Key Archive for the source DataFort, and enter the Recovery Key Archive passphrase. Click Next.

Then browse or enter the path to the Recovery Key Archive for the target DataFort, and enter its passphrase. Click Next.

A message confirms that the keys have been successfully translated.

The LKM UI reflects the new set of translated Cryptainer Keys. Clicking the target DataFort displays all the translated Cryptainers and their identifying information, in red. Each translated Cryptainer is also identified by the word “translated.”

See the section on restoring a Cryptainer in the [DataFort Administration Guide](#).

## TRANSLATING INDIVIDUAL KEYS

The procedure for translating individual keys, or translating keys one at a time, is the same as for translating all the Cryptainer Keys of a DataFort. Key translation can be authenticated either with Recovery Cards or Recovery Key Archives. Either assemble the Recovery Officers and Recovery Cards for both the source DataFort and the target DataFort, or locate the Recovery Key Archives for the source and the target DataFort.

**Note:** See [Key Translation from Previous LKM Versions](#) on page 26 if translating keys from an older version of DataFort.

1. Click the source DataFort in the LKM UI, and in the right pane, right-click a Cryptainer or tape key to be translated. Choose Translate Key (or choose Translate Keys to 2.0 if the source DataFort is a version previous to 2.0 and the target DataFort is 2.0).
2. Select the target DataFort from the drop-down list.
3. Choose the authentication method. Click Next.
4. Follow the screen prompts to translate the keys. When the keys are translated, they can be restored.
5. See the section on restoring a Cryptainer in the [DataFort Administration Guide](#).

## AFTER CRYPTAINER RESTORATION

After restoring Cryptainers, open the LKM UI and click a target DataFort. The right pane shows a new (duplicate) entry for each restored Cryptainer, with updated settings.

The restored Cryptainer shares the Cryptainer Key ID with the translated Cryptainer, but other settings are different. If a translated and restored Cryptainer is active, the formerly red entry will be blue; if it is inactive, it will be gray. Future uploads of the configuration database from the target DataFort will update these settings.

## KEY TRANSLATION FROM PREVIOUS LKM VERSIONS

In the event that LKM must be upgraded to support an upgrade on DataFort, it will also be necessary to ensure that all keys from the old DataFort version are usable with the new LKM.

1. Before upgrading DataFort, access the Back Up Configuration page from the WebUI at **System Config > Recovery > Back Up**, and click the Backup to LKM button. Refer to the [DataFort Administration Guide](#) for details.
2. Set up the new LKM Server (see [Installing LKM Software](#) on page 9).
3. Upgrade the DataFort according to instructions from Decru.
4. Send a new configuration backup to LKM.
5. From LKM, translate all the keys from the old DataFort to the new DataFort.

6. Right-click the DataFort in the LKM menu and select the correct Key Translation option. Depending on the version SAN or NAS, the Key Translation option will show different displays.
  - If translating to a SAN 2.0 DataFort (the FC-Series), select the Translate to 2.0 DataFort option.
  - If translating to a NAS 3.0 DataFort (the E-Series), select the Translate to 3.0 DataFort option.
7. From the drop-down list, choose the target DataFort. The list includes all the DataFort appliances known to the LKM server.
8. Choose the method of authenticating the Key Translation and click Next. Choose Use Recovery Cards unless you have already created a Recovery Key Archive.
  - If you choose Use Recovery Cards, LKM displays the names of the Security Domains of the source and target DataFort appliances. The quorum of Recovery Cards that will be needed (from both DataFort appliances) will be displayed. When prompted to insert Recovery Cards, Recovery Officers insert their Recovery Cards in the smart card reader, and enter their passwords.  
  
Control-click to pre-select the cards you will present, if desired, to speed up the process. Click Next. Follow the prompts to insert each card and enter its password.
  - If you choose Use Recovery Key Archives, browse or enter the path to the Recovery Key Archive for the source DataFort, and enter the Recovery Key Archive passphrase. Click Next.  
  
Then browse or enter the path to the Recovery Key Archive for the target DataFort, and enter its passphrase. Click Next.
9. The LKM UI reflects the new set of translated Cryptainer Keys. Clicking the target DataFort displays all the translated Cryptainers and their identifying information, in red. Each translated Cryptainer is also identified by the word “translated.”

See the section on restoring a Cryptainer in the [DataFort Administration Guide](#).

## IMPORTING AND EXPORTING CRYPTAINER KEYS

---

LKM allows you to selectively export and import Cryptainer Keys and Tape Keys from one LKM server to another. Access is provided through LKM software.

Importing and exporting keys can be helpful when maintaining an offsite clone of a DataFort appliance. LKM can be used to selectively export Cryptainer Keys from the original LKM server and import them to LKM at a remote site.

### CREATING A DATAFORT CLONE

If desired, create a clone of a local DataFort at a remote site, with its own LKM Server. It will then be possible to selectively export keys from the local DataFort to the remote one, using the LKM Servers. To create a DataFort clone, complete the following:

- At the source DataFort, save the configuration database to a file using the Backup Configuration page. Refer to the [DataFort Administration Guide](#) for details.
- Using an uninitialized DataFort, run the Recovery Wizard, accessing the database saved from the source DataFort to initialize the new one. Refer to the [DataFort Administration Guide](#) for details about the Recovery Wizard. This new DataFort can be installed at a remote site as a clone of the source DataFort.
- The new DataFort is now a clone of the source DataFort. It will contain only the key information from the initial database, plus any keys that are exported to it as described below.

### EXPORTING CRYPTAINER KEYS

You can export individual Cryptainer or tape keys or export all the keys associated with a DataFort.

1. At the source LKM server:
  - To export all the keys of a DataFort, right-click a DataFort in the left pane of the LKM UI, and choose Export Keys.
  - To export one Cryptainer Key or tape key, select a DataFort in the left pane of the LKM UI and right-click a Cryptainer or tape key in the right pane. Choose Export Key.
2. Enter and then confirm a passphrase in the dialog that follows.
3. Click Choose Save Location.
4. Specify a location to save the export file. Enter a new filename or accept the default filename (which is based on the DataFort name or key name), and click Save.

### IMPORTING EXPORTED CRYPTAINER KEYS

The saved export file can be imported into another LKM installation.

1. At the target LKM server, choose **File > Import**.
2. Enter the passphrase you supplied when you exported the Cryptainer Keys. Click Choose File Location.
3. Browse to the export file you saved in the previous procedure, and click Open.

The imported keys now appear in the right pane, associated with the appropriate DataFort.



## ■ ■ ■ ■ 4 LKM MANAGEMENT

The main LKM menus contain tools and commands that apply to the LKM server and database. Use these menus for LKM software and data management procedures.

This chapter includes the following topics:

- [Managing the LKM Database](#)
- [Managing LKM Ports](#)
- [DataFort Management](#)
- [Deleting a Cryptainer from LKM](#)
- [Identifying Recovery Cards](#)

## MANAGING THE LKM DATABASE

---

The LKM database can be imported, exported synced between servers or zeroized. See the following topics:

- [Importing the LKM Database](#)
- [Exporting LKM Database](#)
- [Syncing LKM Servers](#)
- [Zeroizing LKM Database](#)

### IMPORTING THE LKM DATABASE

The Import command imports an LKM database that was previously exported as a file, adding the data to the current LKM database. The LKM Database Export file (\*.lkm) may be a complete LKM database or may contain only selected records from an LKM database. You will need to provide the passphrase that LKM used to encrypt the file. You can use the Import menu option for the following:

- To add LKM records from one LKM server to another.  
For example, if you import records to an LKM server in a different Security Domain, the imported records will be merged with the existing records. This works best if you are importing records of different DataFort appliances.
  - To transfer an entire LKM archive from one computer to another (for example, to sync two LKM servers - see [Syncing LKM Servers](#)).
  - To reconstitute an LKM archive from an export file that you created as a backup.
1. Choose **File > Import**.
  2. Click Yes to continue.
  3. Enter the passphrase that was supplied when the LKM Data was exported to a file.
  4. Click Choose File Location.
  5. Enter or browse to the file you wish to import. Click Save.

### EXPORTING LKM DATABASE

The Export command exports the entire LKM Database as a file encrypted with a passphrase. Use the Export command to create a file in order to:

- To add records from one LKM server to another.
  - To move an entire LKM database from one LKM server to another.
  - To back up the LKM database.
1. Choose **File > Export**.
  2. Enter a passphrase that LKM will use to encrypt the export file. Enter it again to confirm.
  3. Click Choose Save Location.
  4. Enter or browse to the directory where you will store the file. Enter a filename and click Save.
  5. Note the filename and the passphrase. You will need them when you are ready to import the file.

## SYNCING LKM SERVERS

If LKM servers are put in operation at the same time, DataFort keeps them in sync. If LKM servers are added later, sync them up once:

- At one LKM server, export the LKM Database (choose **File > Export**).
- At the other LKM server, import the LKM Database exported from the first server (choose **File > Import**).

This ensures that all data is available from both servers. DataFort will keep them in sync thereafter.

## ZEROIZING LKM DATABASE

The Zeroize command clears the contents of the LKM database. Use this command to:

- Avoid duplicate entries if you plan to import an LKM database that includes records for the same DataFort appliances.
- Restore a blank database after you have exported an existing database.

**Note:** If you have any reservations about clearing the database, perform an Export LKM Database command first, so you have a backup file.

1. Choose **File > Zeroize**.  
LKM warns that all the data will be destroyed.
2. Type YES to confirm, and click OK.

## MANAGING LKM PORTS

---

The Edit menu manages LKM server ports. Use this menu to test and configure LKM server ports:

- [Testing LKM Server Ports](#)
- [Configuring the SSL Connection](#)
- [Configuring LKM Server Ports](#)

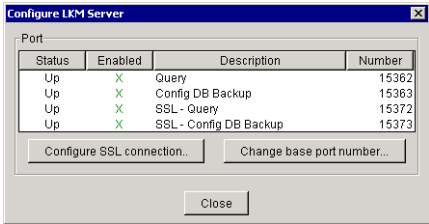
## TESTING LKM SERVER PORTS

The LKM server port configuration can be tested and edited as follows:

- Test the availability of LKM server ports and reporting status
- Configure a secure connection to DataFort appliances (SSL)
- Change the base port number
- Choose **Edit > Port**.

LKM quickly tests LKM server ports for availability.

The results are shown in the Configure LKM Server dialog box. By default, the Query and Config DB Backup ports are enabled, but the two SSL ports are not available until the SSL connection has been configured in LKM.



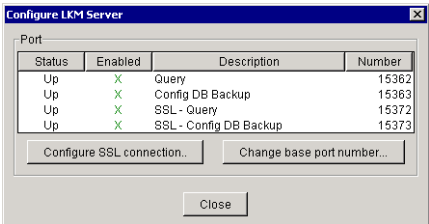
The status of the DataFort Query and DataFort Config DB Backup ports is shown as Up unless there is a port conflict. A status of Configure means that the SSL ports have not yet been configured. The designated port numbers are shown on the right side of the Port window.

**CONFIGURING THE SSL CONNECTION**

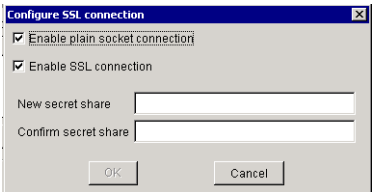
To enable secure communication between DataFort appliances and the LKM server, you must configure the SSL connection at the LKM server, and also enable SSL at one member of each DataFort cluster. It doesn't matter in what order you do this, but secure backups of the configuration database will not proceed until SSL is enabled and the shared secret registered both at the DataFort cluster and the LKM server.

- 1. Choose **Edit > Port**.

A connection test will run. The Configure LKM Server window appears.



- 2. Click Configure SSL Connection. The Configure SSL Connection window appears.
- 3. Click to check the Enable SSL Connection box.
- 4. Enter and confirm the secret that will be used to authenticate the SSL connection. The shared secret can be a string of any characters of any length, including spaces.



A connection test will run. The Configure LKM Server dialog box now shows the status of the SSL ports as Enabled and Up.

5. Click Close.

**Note:** Enable SSL and enter the identical shared secret on DataFort appliances using this instance of LKM as described in the [DataFort Administration Guide](#).

## REQUIRING SSL

It is possible require that communication between DataFort and LKM be SSL communication .

1. Choose **Edit > Port**.

A connection test will run. The Configure LKM Server window appears.

2. Click Configure SSL Connection. The Configure SSL Connection window appears.
3. Click to check the Enable SSL connection and enter and verify the secret share.
4. Click to uncheck the Enable plain socket connection box. Click OK.
5. Verify that only the SSL ports are enabled.
6. Click Close.
7. Make sure that one member of each cluster of DataFort appliances has SSL enabled with the same secret.

## CONFIGURING LKM SERVER PORTS

For communication with connected DataFort appliances the default listening ports on the LKM server are 15362 and 15363. Port 15364 is reserved for internal communication. The ports reserved for secure connection with DataFort appliances are the base port + 10 and base port + 11 (by default ports 15372 and 15373).

In the unlikely event that the LKM server requires these ports for another application, you can configure the LKM server to use a different base port. You must make the same modification for all connected DataFort appliances. To change the base port number:

1. Choose **Edit > Port**.

A connection test will run. The Configure LKM Server window appears.

2. Click Change base port number.
3. Enter the new base port number and click OK.
4. Click Close.

**Note:** Be sure the new base port number is entered on DataFort appliances using this instance of LKM as described in the [DataFort Administration Guide](#).

## DATAFORT MANAGEMENT

---

DataFort appliance configuration databases and records can be managed using the LKM UI. can be See the following topics:

- [Saving Latest DataFort Configuration Database to File](#)
- [Deleting DataFort Records](#)
- [Deleting a DataFort from LKM](#)
- [Marking a DataFort Inactive](#)
- [Opening DataFort WebUI](#)
- [Viewing DataFort Properties](#)

The frequency with which a DataFort appliance backup up its configuration database to LKM can be modified at the DataFort appliance. See [Changing the DataFort Backup Interval](#).

### SAVING LATEST DATAFORT CONFIGURATION DATABASE TO FILE

When a backup of key data to LKM occurs, LKM also saves the most recent version of the DataFort configuration database. If a DataFort has to be restored to its most recent configuration, the Restore Wizard in the DataFort WebUI prompts the administrator to locate a configuration database backup. If this backup is not available, or if all backups were made to LKM, use LKM to create a configuration database file. Once the file has been created, browse to it from the DataFort Restore Wizard.

1. Right-click the DataFort in the list of appliances in the left frame of LKM, and choose Save DB.
2. Browse to the location where you wish to save the file, and enter a filename.
3. Click Save.

### DELETING DATAFORT RECORDS

LKM keeps a cumulative record of Cryptainer and tape keys for all DataFort appliances from which configurations were loaded. After a period of time, the list of DataFort appliances may include units that are no longer in use. If you prefer not to view records of inactive DataFort appliances, LKM gives you two options: [Deleting a DataFort from LKM](#), or [Marking a DataFort Inactive](#).

### DELETING A DATAFORT FROM LKM

1. As a precaution (optional) before you delete, right-click the DataFort in the left or right frame of the LKM window, and choose Properties. Review the properties to verify the identity of the DataFort you intend to delete. Click Close.
2. Right-click the DataFort again, and choose Delete Records.  
You are warned that the information will be deleted permanently from LKM software, and asked if you want to continue.
3. To delete the records, click Yes.

You are alerted to delete the IP address from the LKM Settings page in the DataFort WebUI if this DataFort is still in use. If you do not, the deleted records will be restored with the next automatic update, provided there has been a change to the DataFort configuration.

The DataFort is deleted from the list of DataFort Appliances, together with any Recovery Cards that were associated exclusively with that DataFort.

## MARKING A DATAFORT INACTIVE

If you do not wish to delete any DataFort records from LKM, you can mark inactive DataFort appliances with a red Inactive flag, so you can easily distinguish them in the list. The flag is reversible, and is just a visual sign that you confer—LKM cannot query a DataFort to find out if it is active.

1. Right-click a DataFort in the left or right frame of the LKM window, and choose Mark Inactive.

You are alerted to change LKM settings in the DataFort WebUI if this DataFort is still in use. If you do not, the DataFort will be restored to active status with the next automated update, provided there has been a configuration change.

The DataFort you selected is marked with an Inactive icon.

**Note:** If you right-click the DataFort again, the menu now reads Mark Active. If you choose Mark Active, the Inactive flag is removed.

## OPENING DATAFORT WEBUI

Opening the DataFort WebUI from LKM permits you to log in to a DataFort from the LKM server.

1. Right-click a DataFort in the list on the left side of the LKM main screen, and choose Launch WebUI.

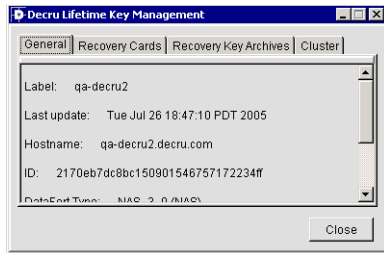
LKM opens Internet Explorer to the domain name listed for the selected DataFort.

2. Log in as administrator and navigate the WebUI as usual.

## VIEWING DATAFORT PROPERTIES

You can view general information that LKM has recorded for a selected DataFort appliance.

1. Right-click a DataFort and choose Properties.
2. Click the tabs to view:
  - The DataFort label that was entered in the DataFort WebUI
  - Date and time the last configuration update was sent to LKM
  - Hostname
  - ID
  - DataFort Type
  - DataFort description
  - Number of Cryptainer Keys known and Number of Cryptainers known
  - Recovery Cards (labels and size of quorum)
  - Known Recovery Key Archives and the dates on which they were created
  - Cluster information, if any



## CHANGING THE DATAFORT BACKUP INTERVAL

By default, DataFort will check its database for changes every 3600 seconds and send key changes to the LKM for storage. To change the interval at which the DataFort appliance sends a backup of its configuration database to a linked LKM appliance:

1. Log in to the DataFort appliance CLI or WebCLI (see the [DataFort Administration Guide](#)).
2. Run the following command on the DataFort CLI:

```
system property set lkm.db.backup.interval <seconds>
```

## DELETING A CRYPTAINER FROM LKM

---

Just as you can delete DataFort records from LKM, you can also delete individual Cryptainer and tape key records. Cryptainer vaults that have been deleted from a DataFort are recorded as a change in DataFort configuration. When LKM updates its database with a new DataFort configuration, it indicates deleted Cryptainer status by graying the name of the Cryptainer in the list in the right frame.

However, you can delete Cryptainer records from LKM entirely, as follows:

1. Select the DataFort in the left pane.
2. From the list of Cryptainers in the right frame, right-click the Cryptainer or tape key you wish to delete, and choose Delete from LKM. You are alerted that the information will be deleted from LKM software, and asked if you want to continue.
3. Click Yes.

The Cryptainer is deleted from the list and from LKM records. LKM reminds you that if this is an active Cryptainer, it will reappear with the next configuration update from that DataFort.

## IDENTIFYING RECOVERY CARDS

---

LKM can identify unmarked or unknown DataFort Recovery Cards.

1. Choose **Recovery > Identify Card** from the LKM menu.
2. When prompted, insert the unidentified Recovery Card in the smart card reader.
3. Click Display Card Details.

LKM displays the card label, its Security Domain, card ID, (and, when applicable, card version).

## ■ ■ ■ ■ 5 LKM TROUBLESHOOTING

If a DataFort does not appear in the list of DataFort Appliances in the LKM UI, or if its records are not being updated, or if an LKM alert appears on the DataFort Home page, check the following:

**Communication Ports** If you have set up a DataFort for automatic backup to the LKM server, make sure that the same ports were specified on the LKM server. Choose [Edit > Port](#) to check the number of the base port. If the port is not responding, change the base port number. If the number is doesn't match the number registered with DataFort, enter a matching base port. For more information, see [Managing LKM Ports](#) on page 31.

If one of the ports is down, try restarting the server port. If the error persists, it means some other application is using one of the LKM ports. Either choose to use another set of ports for LKM (by changing the base ports to unused ports) or re-configure the other application.

When using a Windows XP server, you must configure Windows Firewall as follows: From the Windows Control Panel, select Windows Firewall. Click the Exceptions tab and add the ports used by LKM by clicking Add port. Add ports 15362 and 15363 for clear communication and ports 15372 and 15373 for SSL. Restart LKM.

**SSL Communication** Secure automatic backup using SSL must be explicitly enabled in LKM as well as in connected DataFort appliances. For secure backup to the LKM server, make sure that SSL is enabled and configured with the same base port and shared secret at both parties to the connection.

When using a Windows XP server with SSL, you must configure Windows Firewall as follows: From the Windows Control Panel, select Windows Firewall. Click the Exceptions tab and add the ports used by LKM by clicking Add port. Add ports 15362 and 15363 for clear communication and ports 15372 and 15373 for SSL. Restart LKM.

**Log Files** Every time a configuration database backed up to the LKM server, LKM creates a log entry in a file named LKM.log, which is also found in the LKM application folder. Open the log file with any text editor to check the status of a particular configuration database loading operation. The log file lkmService.log contains more detailed information from the LKM service.

## INDEX

### A

- Archiving Tools
  - Generate Cryptainer Key File 23
  - Generate Recovery Key Archive 21

### B

- backup frequency to LKM 11

### C

- changing DataFort configuration backup interval 36
- cloned DataFort 28
- Communication Ports 37
- Configuring the SSL Connection 32
- Cryptainer Key 5, 14, 25
- Cryptainer Key File 23
- Cryptainers
  - color-coding in UI 14

### D

- Data Recovery Tool
  - Identify Recovery Card 36
- DataFort Properties 10, 35
- Delete Cryptainer from LKM 36
- Delete DataFort Records 34

### E

- Export Cryptainer Keys 28

### G

- Generate Cryptainer Key File 23
- Generate Recovery Key Archive 21

### I

- Identify Recovery Card 36
- Import Cryptainer Keys 28

### K

- key escrow 11
- key expiration 15
- Key Limits 6
- key translation 25
- Key translation from previous LK versions 26
- keys in LKM 13

### L

- LKM Database
  - clear 31
  - export 30
- LKM Ports 31
- LKM server
  - port configuration 33
  - sync 31
- LKM server requirements 7
- LKM settings
  - specify for DataFort 10
- LKM software
  - accessing 10
  - controlling the display 13
  - installing 9
  - tools and options 17
- LKM UI 10, 11
- LKM Windows Service 11

### M

- Marking a DataFort Inactive or Active 35
- Microsoft SQL Server 8, 9
- MySQL 8, 9
- MySQL version installed 9

### N

- number of keys in LKM displayed 13
- number of LKM servers 6

### O

- Open DataFort WebUI 35

### P

- Pool Key 15
- purge keys 6

### R

- Recovery Cards 36
- Recovery Key Archive 21
- require SSL 33
- reset Windows Service 11

### S

- Save Latest Configuration Database to File 34
- secure communication, configuring 32
- server ports 7

SQL Server 8

SSL 37

- communication 37

- configuring 32

- connection 32

- require connection 33

status bar 13

## **T**

Tape Key 5, 14, 15, 25

## **U**

upgrading LKM 26

## **W**

Windows Firewall 37

Windows Service 11